REMARKS

1. Claims 1 – 8 stand rejected under 35 USC § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. Claims 1 – 8 have been canceled from the Application, rendering the current rejection moot.

2. Claim 9 stands rejected under 35 USC § 101 as being directed to non-statutory subject matter. Claim 9 has been canceled from the Application, rendering the current rejection moot.

3. Claims 1, 2, 4 – 11 and 13 – 17 stand rejected under 35 USC 102(b) as being anticipated by Schneier, pp 574 – 576. To describe the invention with greater clarity, Applicant has added new Claims 18 – 39, with Claims 1 – 17 being canceled. Thus, the current rejection is rendered moot.

4. Claims 3 and 12 stand rejected under 35 USC 103(a) as being unpatentable over Schneier, pp. 574 and 186 and further in view of the Examiner's Official Notice that the provision of information in a certificate authenticating a third certificate is old and well known in the art. Applicant expressly reserves to itself the right to request that the Examiner provide a reference in support of her finding, or in the alternative, an affidavit, should she apply such finding in future rejections. Otherwise, the current rejection is rendered moot by the cancellation of Claims 3 and 12 from the application.

CONCLUSION

In view of the above, there remain no outstanding issues. Therefore, the Examiner is earnestly requested to withdraw all rejections and allow the Application to pass to issue as a U.S. Patent. Should the Examiner have any questions regarding the invention, she is urged to contact the Applicant's attorney at the telephone number given below.

Respectfully submitted,

Michael A. Glenn
Reg. No. 30,176

Customer No. 22862

AMENDMENTS (MARKED-UP COPY)

Please add new Claims 18 – 39 as follows:

18. A method of modifying and distributing trust information, including the steps of:

providing a plurality of parties, said parties defining a hierarchy;

providing additional entities;

defining trust relationships by a party with other parties and, optionally, with at least one of said additional entities within parameters set by at least one higher party;

distributing trust information for said hierarchy from a top-level authority;

receiving said trust information by a client; and

validating said trust information by said client.

19. A method as in Claim 18, wherein said step of defining trust relationships by a party in said hierarchy comprises the steps of:

receiving a root certificate from any of a child in said hierarchy and an additional entity;

generating a fingerprint of said root certificate;

incorporating said fingerprint into a root security information object (RSIO), said RSIO including a root certificate of said party;

setting trust information for any of said child and said additional entity;

setting delegation information for any of said child and said additional entity; and

providing said RSIO to a parent in said hierarchy.

20. A method as in Claim 19, wherein said fingerprint comprises a digest of a signature in said root certificate.

21. A method as in Claim 19, wherein said step of defining trust information comprises the step of:

setting trust information for said child and said additional entity in a trust vector, said trust vector including a plurality of bits, wherein each bit designates a role.

22. A method as in Claim 19, wherein said step of setting delegation information comprises the step of;

setting delegation information for said child and said additional entity in a delegation vector, said delegation vector including a plurality of bits, wherein each bit designates a corresponding trust vector bit, said delegation information specifying whether said corresponding trust vector bit may be set by a party lower in the hierarchy.

23. A method as in Claim 19, wherein said step of distributing security information comprises the steps of:

linking said RSIO's to form a hierarchic security information object (HSIO); and

distributing said HSIO.

24. A method as in Claim 23, wherein said step of linking said RSIO's comprises:

matching a child's fingerprint in a parent's RSIO with the child's root certificate in the child's RSIO.

25. A method as in Claim 23, wherein said step of receiving said trust information comprises:

receiving said HSIO; and

receiving one of a root certificate and a chain of root certificates from said top-level authority.

26. A method as in Claim 23, wherein said step of validating said trust information comprises the steps of:

for each level of said hierarchy:

checking validity date of a child's RSIO in said HSIO;

validating a signature in said child's RSIO against a signature in said child's root certificate; and

checking that said child's fingerprint is contained in said parent's RSIO.

27. A method as in Claim 26, wherein said top-level authority's trust information is validated against said received root certificate or chain or root certificates.

28. A method as in Claim 18, further comprising the step of:

updating said trust information.

29. A computer program product for modifying and distributing trust information, said computer program product comprising a tangible medium having computer readable program code means embodied thereon, comprising computer readable program code for:

providing a plurality of parties, said parties defining a hierarchy;

providing additional entities;

defining trust relationships by a party with other parties and, optionally, with at least one of said additional entities within parameters set by at least one higher party

distributing trust information for said hierarchy from a top-level authority;

receiving said trust information by a client; and

validating said trust information by said client.

30. A computer program product as in Claim 29, wherein said computer program code for defining trust relationships by a party in said hierarchy comprises computer program code for:

receiving a root certificate from any of a child in said hierarchy and an additional entity;

generating a fingerprint of said root certificate;

incorporating said finger print into a root security information object (RSIO), said RSIO including a root certificate of said party;

setting trust information for any of said child and said additional entity;

setting delegation information for any of said child and said additional entity; and

providing said RSIO to a parent in said hierarchy.

31. A computer program product as in Claim 30, wherein said fingerprint comprises a digest of a signature in said root certificate.

32. A computer program product as in Claim 30, wherein said computer program code for defining trust information comprises computer program code for:

setting trust information for said child and said additional entity in a trust vector, said trust vector including a plurality of bits, wherein each bit designates a role.

33. A computer program product as in Claim 30, wherein said computer program code for setting delegation information comprises computer program code for;

setting delegation information for said child and said additional entity in a delegation vector, said delegation vector including a plurality of bits, wherein each bit designates a corresponding trust vector bit, said delegation information specifying whether said corresponding trust vector bit may be set by a party lower in the hierarchy.

34. A computer program product as in Claim 30, wherein said computer program code for distributing security information comprises computer program code for:

linking said RSIO's to form a hierarchic security information object (HSIO); and

distributing said HSIO.

35. A computer program product as in Claim 34, wherein said computer program code for linking said RSIO's comprises computer program code for:

matching a child's fingerprint in a parent's RSIO with the child's root certificate in the child's RSIO.

36. A computer program product as in Claim 34, wherein said computer program code for receiving said trust information comprises computer program code for:

receiving said HSIO; and

receiving one of a root certificate and a chain of root certificates from said top-level authority.

37. A computer program product as in Claim 34, wherein said computer program code for validating said trust information comprises computer program code for:

for each level of said hierarchy:

checking validity date of a child's RSIO in said HSIO;

validating a signature in said child's RSIO against a signature in said child's root certificate; and

checking that said child's fingerprint is contained in said parent's RSIO.

38. A computer program product as in Claim 37, wherein said top-level authority's trust information is validated against said received root certificate or chain or root certificates.

39. A computer program product as in Claim 29, further comprising computer program code for:

updating said trust information.

Please cancel Claims 1 – 17 from the application.